Notice of Allowability	Application No.	Applicant(s)	
	10/080,574	BEAVERS, JOHN B.	
	Examiner	Art Unit	
	Nirav Patel	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Appeal Brief filed 6/05/06*.

2. ☒ The allowed claim(s) is/are *1-12 and 14-22*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 12/22/05
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20060811* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with the applicant representative, Mr. Hodgson Serge J. (Registration No. 40,017) on 8/17/2006.

CLAIMS:

a. Referring to claim 1:

Please replace claim 1 as follows:

A method of producing at least one alert indication based on a number of events derived from an enterprise comprising:

providing a plurality of enterprise device outputs, at least a portion of the outputs having different formats, each output containing an event relating to an enterprise device;

translating each output into a common format event comprising:

matching data values in the device output with a signature specification for each enterprise device, the signature specification containing:

a number of signatures; a first location identifier for each signature; and

a first key;

wherein the signature is a listing of names found in the device output, the first location identifier determines the method used to locate the name in the device output, and the first key determines where to locate the name in the device output;

identifying a message type from a plurality message types for each enterprise device based on the device output as part of the translated common format event;

adding knowledge to the common format event using knowledge base table files to generate a knowledge-containing common format event;

applying one or more rules from a set of rules to the knowledge-containing common format event to generate the alert indication; and

generating the alert indication, wherein the alert indication includes at least a text message describing the event contained in the output of the enterprise device.

b. Referring to claim 5:

Please replace claim 5 as follows:

The method of claim 1, wherein the translating step further comprises:

producing the remainder of the translated common format event in argument name and argument value pairs using an argument specification, the argument specification containing;

a listing of arguments;

a field type;

a second location identifier for each argument; and

a second key;

wherein each argument is a listing of argument names for inclusion in the translated common format event, the field type specifies the form of an argument value found in the device output, the second location identifier determines the location of each argument value, and the second key locates the argument value in the device output to be displayed with the argument name.

c. Referring to claim 10:

Please replace claim 10 as follows:

The method of claim 3, wherein the translating step further comprises:

producing the remainder of the translated common format event in argument name and argument value pairs using an argument specification, the argument specification containing;

a listing of arguments;

a field type;

a second location identifier for each argument; and

a second key;

wherein each argument is a listing of argument names for inclusion in the translated common format event, the field type specifies the form of an argument value found in the device output, the second location identifier determines the location of each

argument value, and the second key locates the argument value in the device output to be displayed with the argument name.

d. Referring to claim 13:

Please cancel claim 13.

e. Referring to claim 14:

Please replace claim 14 as follows:

The method of claim 1, wherein a threat level is included as part of the alert indication.

f. Referring to claim 15:

Please replace claim 15 as follows:

A system for producing at least one alert indication based on a number of events derived from an enterprise comprising:

a plurality of enterprise devices, each device capable of producing an output;

a number of translation files, the translation files allowing the output to be translated into a common format event, the translation comprising:

matching data values in the device output with a signature specification for each enterprise device, the signature specification containing:

a number of signatures; a first location identifier for each signature; and

a first key;

wherein the signature is a listing of names found in the device output, the first location identifier determines how to locate the name in the device output, and the first key determines where to locate the name in the device output;

identifying a message type from a plurality message types for each enterprise device based on the device output as part of the translated common format event;

a number of knowledge base table files, matching of the common format event with one or more of the knowledge base table files adding knowledge from the matched file to generate a knowledge-containing common format event;

a number of rule files, the rule files governing generation of the alert indication; and

a rules processor for generating the alert indication, wherein the alert indication includes at least a text message describing the event contained in the output of the enterprise device.

Response to Arguments

3. Applicant's arguments, filed June 05 2006 have been fully considered and are persuasive.

Allowable Subject Matter

4. Claims 1-12 and 14-22 are allowed.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 12/22/05 was filed after the mailing date of the Final Office Action on 12/21/05. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO

Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NBP
8/17/06

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100